IN THE CLAIMS

1. (Previously presented) An access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the access controller comprising:

an access restriction module configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition list of the access controller;

an input module configured to input user information corresponding to the access prohibited user; and

a list update module configured to update the access prohibition list of each access controller connected with the network, according to the user information input through the input module.

2. (Previously presented) An access controller in accordance with claim 1, wherein the list update module sends out to the other access controllers a

registration instruction to register the input user information on the access prohibition list of the other access controllers.

3. (Previously presented) An access controller in accordance with claim 1, wherein the list update module sends out an updated access prohibition list to the other access controllers.

4. (Previously presented) An access controller in accordance with claim 1, wherein the access interception module also intercepts an access that has not been completed.

5. (Previously presented) An access controller in accordance with claim 1, further comprising an access control list update module configured to update the access control list according to the access prohibition list.

6. (Original) An access controller in accordance with claim 5, wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

7. (Original) An access controller in accordance with claim 6, wherein the predetermined timing is after the update of the access control list has been completed.

8. (Previously presented) An access controller in accordance with claim 6, wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed.

9. (Previously presented) An access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the access controller comprising:

an access restriction module configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

a receiving module configured to receive user information of an access prohibited user, from one of the other access controllers connected to the network ;

a list update module configured to update the access prohibition list of the access controller, which records user information of access prohibited users, according to the received user information; and

an access interception module configured to restrict the access by reference to the access prohibition list prior to the access control list.

10. (Previously presented) An access controller in accordance with claim 9, wherein the access interception module also intercepts an uncompleted access.

11. (Previously presented) An access controller in accordance with claim 9, further comprising an access control list update module configured to update the access control list according to the access prohibition list.

12. (Original) An access controller in accordance with claim 11, wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

13. (Original) An access controller in accordance with claim 12, wherein the predetermined timing is after the update of the access control list has been completed.

14. (Previously presented) An access controller in accordance with claim 12, wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed.

15. (Previously presented) An access control system in which a plurality of storage devices for storing information resources and access controllers for controlling accesses to the information resources stored in the storage devices are connected with a network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, each access controller comprising:

an access restriction module configured to restrict access to each information resource stored in a storage device and listed on the an access control list of the access controller that records access right to each information resource; and

an access interception module configured to restrict the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users, prior to the access control list;

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or the updated access prohibition list to the other access controllers in response to the update; and

the other access controllers further comprising a list update module configured to receive the user information or the updated access prohibition list and

to update the access prohibition list thereof to include the received user information or updated access prohibition list.

16. (Previously presented) An access control system in accordance with claim 15, wherein the distribution module broadcasts the user information or the updated access prohibition list over all of the other access controllers.

17. (Previously presented) An access control system in accordance with claim 15, wherein the distribution module of each access controller sends out the user information or the updated prohibition list to a predetermined other one of the access controllers, thereby transmitting the user information or the updated prohibition list from one access controller to another.

18. (Previously presented) An access control system in which a plurality of storage devices for storing information resources stored in the storage devices and access controllers for controlling an access to the information resources are connected with a network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, each access controller comprising:

an access restriction module configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

an access interception module configured to restrict the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users, prior to the access control list;

a distribution module configured to broadcast the user information to the other access controllers in response to update of its own access prohibition list;

a list update module configured for the access controller to update its own access prohibition list in response to receiving the user information;

an access control list update module configured to update the access control list of the access controller to include the received user information after updating the access prohibition list; and

a user information deletion module configured to delete the user information from the access prohibition list after updating the access control list.

19. (Previously presented) An access control method for controlling an access to an information resource stored in a storage device connected to an access controller via a network, the method being executed by the access controller in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices

is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the method comprising the steps of:

restricting access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

intercepting an access by an access prohibited user listed on the access prohibition list of the access controller;

inputting user information corresponding to the access prohibited user; and

updating the access prohibition list of each access controller connected with the network, according to the input user information.

20. (Previously presented) An access control method for controlling an access to an information resource stored in a storage device connected to an access controller via a network, the method being executed by the access controller in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any

information resource stored in the storage devices, the method comprising the steps of:

restricting access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

receiving user information of an access prohibited user from one of the other access controllers connected to the network;

updating the access prohibition list of the access controller on which user information of access prohibited users is recorded, according to the received user information; and

restricting the access by reference to the access prohibition list prior to the access control list.

21. (Previously presented) An access control method for controlling an access to information resources stored in storage devices in an access control system where a plurality of storage devices for storing information resources and access controllers are connected with a network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the method comprising the steps of:

each access controller restricting access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

each access controller restricting the access by reference to the access prohibition list of the access controller, which records user information of access prohibited users, prior to the access control list;

at least one of the access controllers having the updated access prohibition list sending out the user information or the updated access prohibition list to the other access controllers in response to the update; and

the other access controllers receiving the user information or the updated access prohibition list and updating the access prohibition list thereof to include the received user information or updated access prohibition list.

22. (Previously presented) A computer readable recording medium in which is stored a computer program executed by an access controller to control an access to an information resource stored in a storage device connected to the access controller via a network, the computer program being executed in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access

prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the computer program comprising:

a first program code for restricting access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

a second program code for intercepting an access by an access prohibited user listed on the access prohibition list of the access controller;

a third program code for inputting user information corresponding to the access prohibited user; and

a fourth program code for updating the access prohibition list of each access controller connected with the network, according to the input user information.

23. (Previously presented) A computer readable recording medium in which is stored a computer program executed by an access controller to control an access to an information resource stored in a storage device connected to the access controller via a network, the computer program being executed in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the computer program comprising:

a first program code for restricting access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded;

a second program code for receiving user information of an access prohibited user from one of the other access controllers connected to the network;

a third program code for updating the access prohibition list of the access controller on which user information of access prohibited users is recorded, according to the received user information; and

a fourth program code for restricting the access according to the access prohibition list prior to the access control list.

24. (Previously presented) An access controller, comprising:

an access restriction module configured to restrict access to an information resource stored in a storage device, by referring to an access controller on which an access right to the information resource is recorded;

an access interception module configured to refer to an access prohibition list on the access controller and to intercept an access by a user listed on the access prohibition list;

an input module configured to input prohibited user information of a prohibited user to be added to the access prohibition list; and

a list update module configured to receive the prohibited user information input through the input module and to update the access prohibition list with the received prohibited user information;

wherein the list update module sends an output via a network to a plurality of access controllers connected to a plurality of storage devices, to reflect the received prohibited user information on an access prohibition list of each of the access controllers to which the output is sent, so that the access prohibition list of the access controller having the list update module and the access prohibition lists of the access controllers receiving the output from the list update module all contain the received prohibited user information; and

wherein the access controller further comprises an access control list update module configured to update the access control list with the prohibited user information on the access prohibition list, and to delete the prohibited user information from the access prohibition list after updating the access control list stored therein.

25. (Previously presented) An access controller in accordance with claim 24,

wherein the output sent by the list update module is a registration instruction to each of the access controllers connected via the network, to register the received prohibited user information on the access prohibition list thereof.

26. (Previously presented) An access controller in accordance with claim 24,

wherein the output sent by the list update module is an updated access prohibition list.

27. (Previously presented) An access control method for controlling an access to an information resource stored in a storage device connected to an access controller via a network, the method being executed by the access controller in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices, the method comprising the steps of:

restricting access to an information resource stored in a storage device, by referring to an access controller on which an access right to the information resource is recorded;

referring to an access prohibition list on the access controller to intercept an access by a user listed on the access prohibition list;

inputting prohibited user information of a prohibited user to be added to the access prohibition list;

receiving the prohibited user information input through the input module to update the access prohibition list with the received prohibited user information;

sending an output via the network to the access controllers connected thereto, to reflect the received prohibited user information on the access prohibition list of each of the access controllers to which the output is sent, so that the access prohibition lists of the sending access controller and of the access controllers receiving the output from the sending access controller all contain the received prohibited user information;

updating the access control lists of the sending access controller and of the receiving access controllers with the prohibited user information on the access prohibition lists thereof; and

deleting the prohibited user information from the access prohibition lists of the sending and receiving access controllers after updating the access control lists stored therein.

28. (Previously presented) A computer readable recording medium in which is stored a computer program executed by an access controller to control an access to an information resource stored in a storage device connected to the access controller via a network, the computer program being executed in a system where a plurality of the access controllers and storage devices are connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access

prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

the computer program comprising:

a first program code for restricting access to an information resource stored in a storage device, by referring to an access controller on which an access right to the information resource is recorded;

a second program code for referring to an access prohibition list on the access controller to intercept an access by a user listed on the access prohibition list;

a third program code for inputting prohibited user information of a prohibited user to be added to the access prohibition list;

a fourth program code for receiving the prohibited user information input through the input module to update the access prohibition list with the received prohibited user information;

a fifth program code for sending an output via the network to the access controllers connected thereto, to reflect the received prohibited user information on the access prohibition list of each of the access controllers to which the output is sent, so that the access prohibition lists of the sending access controller and of the access controllers receiving the output from the sending access controller all contain the received prohibited user information;

a sixth program code for updating the access control lists of the sending access controller and of the receiving access controllers with the prohibited user information on the access prohibition lists thereof; and

a seventh program code for deleting the prohibited user information from the access prohibition lists of the sending and receiving access controllers after updating the access control lists stored therein.